

## 資料使用者對保障個人資料私隱的態度調查 2020

### 調查摘要

#### 引言

1. 個人資料私隱專員公署（私隱公署） 委託香港大學社會科學研究中心於 2020 年 8 月至 10 月期間，進行一項資料使用者對個人資料私隱的態度的意見調查，為私隱公署提供有關個人資料私隱的最新資訊以作參考。

#### 調查方法

2. 本次調查一共收到 227 個回應，其中 203 個是透過電話進行的問卷調查，其餘 24 個是透過網上進行的問卷調查。基於回應率不高，調查結果未能被推算為涵蓋香港所有資料使用者。但就行業及香港僱員人數而言，調查結果集合來自不同行業的資料使用者的意見，在分析資料使用者對資料保障及私隱的看法方面，仍具有一定價值。

#### 主要調查結果

##### 受訪者背景

3. 調查收集到的回應來自 13 個不同行業，因此樣本具廣泛代表性。由於回應率不高，所得的結果未足以確定在統計學上的代表性，所以樣本沒有被加權調整至與政府統計處的資料相配。然而，回應所包含的行業廣泛，有助了解不同行業的意見。雖然小型公司（即在香港有 1-9 名僱員的公司）在本調查的樣本中佔多數，但樣本中亦包含各類規模的公司。

##### 私隱管理系統

4. 在對私隱管理系統的了解程度方面，最多受訪者（25%）回答完全不了解（在 0 至 10 分中給予 0 分；0 分代表完全不了解，10 分代表完全了解），

但 37.9%的受訪者給予 6 分或以上。在實施私隱管理系統的階段方面，最多受訪者（27.3%）回答完全沒有實施（評分為 0），但 49.7%的受訪者的回答評分為 6 分或以上。被問到私隱管理系統的主要好處，最多受訪者（共 70 個回應）表示是更佳的資料保障，其次是更能達至合規（共 5 個回應），而其他的回答只有一至兩個回應。被問到實施私隱管理系統的主要困難，最多受訪者（共 7 個回應）認為是教育僱員，其次是欠缺管理層的支持（共 4 個回應）及私隱管理系統的要求欠缺清晰（共 3 個回應）。

### 保障資料主任

5. 只有 17.6%的受訪者有委任保障資料主任。

### 私隱影響評估

6. 只有 14.1%的受訪者曾進行私隱影響評估。

### 合規與投訴

7. 關於在遵從《個人資料（私隱）條例》（《私隱條例》）方面的困難程度（在 0 至 10 分中評分；0 為完全沒有困難，10 為非常困難），最多受訪者（21.4%）給予 5 分，而 21.4%的受訪者回答 6 至 10 分。被問到過去 12 個月接獲與私隱相關的投訴數目，絕大多數受訪者（94.6%）表示未曾接獲投訴，而平均每間機構接獲的投訴數目為 40，這顯示大部分的投訴只與個別資料使用者有關。

### 對中國內地相關法規的認識

8. 大部分受訪者不認識中國內地兩條有關保障個人資料的法規，超過一半受訪者表示對《網絡安全法》（58.9%）及《個人信息安全規範》（59.0%）完全不認識（在 0 至 10 分中給予 0 分；0 為完全不認識，10 為非常熟悉）。

### 對私隱公署的認識

9. 受訪者被問到有否透過大眾媒體、大眾媒體以外的廣告、刊物、網站/社交媒體及活動接觸到私隱公署的推廣訊息。過半受訪者（59%）表示透過大

眾媒體認識私隱公署，其次是透過大眾媒體以外的廣告（28%）、網站/社交媒體（25%）、刊物（24%）及活動（12%）。被問到私隱公署提供哪種額外支援是最為有效的，最多受訪者（共 27 個回應）表示私隱公署應加強推廣/宣傳，尤其是網上推廣/宣傳；其次是提供免費或網上培訓（共 13 個回應）及更有效地分發刊物（共 10 個回應）。

### 對修訂《私隱條例》的支持度

10. 本研究涵蓋《私隱條例》的 7 項主要修訂建議。針對重大的資料外洩事故（例如國泰航空的資料外洩事故），相關修例建議包括：(1) 要求機構通報私隱公署；(2) 賦權私隱公署規定機構通知客戶及(3) 罰款。針對重大濫用個人資料（例如起底），考慮的修訂包括：(4) 要求由香港機構控制的社交媒體平台及網站刪除有關內容；(5) 要求從受海外控制的社交媒體平台及網站刪除有關內容；(6) 賦予公署刑事調查的權力及(7) 賦予公署對此類個案提起訴訟的權力。受訪者對這 7 項修訂的支持程度頗高，超過 80% 的受訪者對 3 項有關資料外洩事故的修例建議的評分為 6 或以上（在 0 至 10 分中評分，0 為完全不支持，10 為完全支持），其中超過 60% 的受訪者完全支持有關通知的修訂及超過 45% 的受訪者完全支持有關罰款的修訂。另外，超過 60% 的受訪者對 4 項有關起底的修訂的評分為 6 或以上，其中約 30% 完全支持全部四項修訂。
11. 而網上調查特別涵蓋額外 11 項《私隱條例》的修訂建議，包括：(1) 指明保留資料的期限；(2) 規管資料處理者；(3) 釐清個人資料的定義；(4) 加入對私隱保障問責的法例要求；(5) 加強監管敏感個人資料；(6) 加強保障兒童個人資料；(7) 更新對跨境/邊界個人資料轉移的規管；(8) 加入被遺忘權；(9) 加入對自動化決策的反對權；(10) 加入資料可攜權及(11) 廢除資料使用者申報計劃。因網上調查主要由私隱公署的保障資料主任聯會的會員完成，預料他們相對較了解修例背後的原因。在網上調查中，至少 70% 的受訪者對全部 11 項修例建議的支持程度給予 6 分或以上（在 0 至 10 分中評分，0 為完全不支持，10 為完全支持）。其中，至少 40% 的受訪者完全支持釐清個人資料的定義、加強保障敏感個人資料及兒童的個人資料的建議。此

外，至少 30%的受訪者完全支持規管資料處理者、加入私隱保障問責、加強個人資料轉移的跨境/邊界保障、加入被遺忘權、加入有關自動化決策的權利及廢除資料使用者申報計劃的建議。同時，亦有至少 20%的受訪者完全支持資料保留政策及可攜權的建議。

### 新科技的應用情況及私隱風險

12. 網上調查特設有關人工智能、大數據、區塊鏈、雲端運算及物聯網的應用情況的問題，及受訪者對這些新資訊及通訊科技的相關私隱風險的看法，包括過度收集個人資料、缺乏透明度、未經同意下更改個人資料用途、資料保安風險及不必要地保留個人資料。在應用情況方面，雲端運算（50%的受訪者已採用）及物聯網（41.7%的受訪者已採用）的應用比率是最高。再次強調，因網上調查主要由保障資料主任聯會的會員完成，估計他們相對較了解這些新資訊及通訊科技的相關私隱風險。受訪者普遍認為人工智能及大數據涉及較高私隱風險，特別是過度收集個人資料（人工智能 64.3%，大數據 62.5%）、處理個人資料缺乏透明度（人工智能 57.1%，大數據 50.0%）、未經同意更改個人資料用途（人工智能 57.1%，大數據 50.0%）、不必要地保留個人資料（人工智能 47.1%，大數據 43.8%），以及資料保安風險（人工智能 50.0%，大數據 43.8%）。

## 建議

### 私隱管理系統

13. 儘管超過三分之一的受訪者對私隱管理系統的了解程度給予 6 分或以上，但仍約有四分之一的受訪者表示完全不了解，這顯示有需要更廣泛地教育機構有關私隱管理系統的概念，使它們至少能明白其相關性。私隱管理系統實施的情況亦與上述脗合，約有四分之一的受訪者表示全完沒有實施。不過，大部分受訪者清楚明白私隱管理系統的主要好處是最佳的資料保障。而最多受訪者面對的困難是教育僱員，同樣顯示有需要提供更多培訓。



### 保障資料主任及私隱影響評估

14. 少於 20% 的受訪者有委任保障資料主任或曾進行私隱影響評估，顯示有需要進一步向機構述明就委任保障資料主任及進行私隱影響評估帶來的好處。

### 合規與投訴

15. 關於遵從《私隱條例》的困難程度，受訪者的回應都有很大差異，這顯示有需要找出面對較大困難的行業（私隱公署接獲的投訴數字應可為有關工作提供良好的基礎）。由於絕大部分的受訪者表示未曾接獲有關私隱的投訴，這顯示大部分的投訴只涉及少數資料使用者，因此在這方面的工作需繼續採取更具針對性的方法。

### 對中國內地有關資料保障的法規的認識

16. 大部分受訪者表示不認識中國內地兩條主要關於資料保障的法規，雖然研究未有問及兩條法規是否與受訪者本身的工作相關，但亦可探討是否有需要舉辦具針對性的培訓。

### 對私隱公署的認識

17. 最多受訪者透過大眾媒體接觸到私隱公署的推廣訊息，其次是大眾媒體以外的廣告、網站/社交媒體、刊物及活動，這顯示私隱公署或需考慮更新宣傳策略。尤其在有關私隱公署可給予的額外支援，最多受訪者認為應加強推廣/宣傳，特別是在網上的推廣/宣傳；其次是提供免費或網上培訓及更有效地分發刊物。

### 對修例建議的支持

18. 受訪者對於涉及重大的資料外洩事故及重大濫用個人資料（例如起底）的 7 項《私隱條例》修訂建議都有較高的支持度，特別是有關發生重大的資料外洩事故（例如國泰航空的資料外洩事故）時須通報私隱公署和通知客戶及罰款方面的建議，而受訪者對於 4 項涉及起底的修例建議的支持度則相對較低。

19. 網上調查特別涵蓋額外 11 項《私隱條例》修例建議。儘管 11 項修例建議都獲得頗高的支持度，因網上調查主要由保障資料主任聯會的會員完成，在詮釋有關結果時需更為審慎。然而，有關釐清個人資料的定義、加強保障敏感個人資料及兒童的個人資料的修例建議獲最多受訪者表示完全支持，這顯示這些修例建議或許可獲優先處理，而對保障個人資料私隱較有認識的資料使用者亦有較大機會支持這些修訂。相對而言，有關規管資料處理者、加入私隱保障問責、加強個人資料跨境/邊界轉移的保障、加入被遺忘權、有關自動化決策的權利及廢除資料使用者申報計劃的修例建議所獲得的支持度相對較低。資料保留政策及可攜權所獲得的支持度則是最低。

#### 新科技的實施階段及私隱風險

20. 從網上調查可見，最多受訪者已採用的新科技是雲端運算及物聯網。不過，約半數受訪者認為人工智能及大數據一般在過度收集個人資料、處理個人資料的透明度、未經同意下更改個人資料用途、不必要地保留個人資料及資料保安方面都涉及較高的私隱風險，這顯示高私隱風險可能是導致這些新資訊及通訊科技在實施方面較為落後，因此私隱公署在這方面的指引將更為重要。

2020 年 1 月 28 日